

(21) Application No: **0420423.6**

(22) Date of Filing: **14.09.2004**

(71) Applicant(s):  
**IGT**  
**(Incorporated in USA - Nevada)**  
**9295 Prototype Drive, Reno,**  
**Nevada 89521, United States of America**

(72) Inventor(s):  
**Michael P Coppert**

(74) Agent and/or Address for Service:  
**J A Kemp & Co.**  
**14 South Square, Gray's Inn, LONDON,**  
**WC1R 5JJ, United Kingdom**

(51) INT CL:  
**G06F 11/34 (2006.01)** **G06F 11/07 (2006.01)**  
**G06F 11/32 (2006.01)**

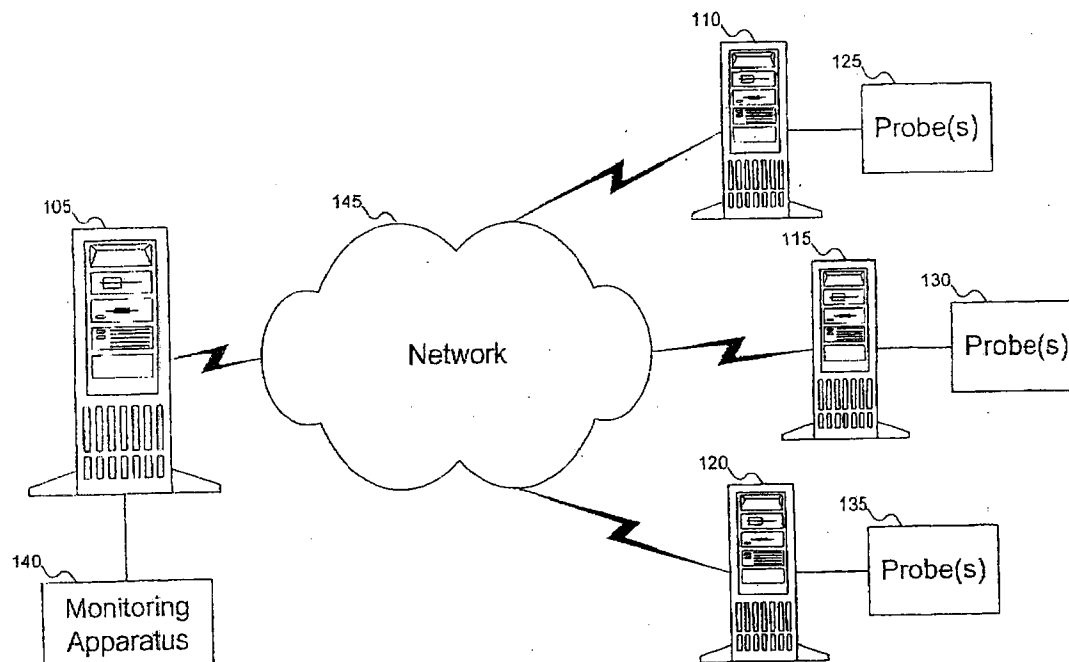
(52) UK CL (Edition X ):  
**G4A AFMD AFML**

(56) Documents Cited:  
**WO 2004/088604 A1** **WO 2003/090085 A2**  
**WO 2000/065448 A1** **US 6636983 B1**  
**US 5796633 A** **US 5726912 A**

(58) Field of Search:  
INT CL<sup>7</sup> **G06F**  
Other: **ONLINE: EPODOC, WPI, JAPIO**

(54) Abstract Title: **Monitoring computer system software**

(57) A probe 125, 130, 135 detennines a value for a metric for a site 110, 115, 120. A message is generated including the value for the metric, and is delivered to a monitoring apparatus 140 at a central (or remote) site 105. The monitoring apparatus determines if the value is acceptable, based on the metric and possibly the site that the probe is monitoring. If the value is not acceptable, then the monitoring apparatus displays an alert to a possible problem.



**FIG. 1**

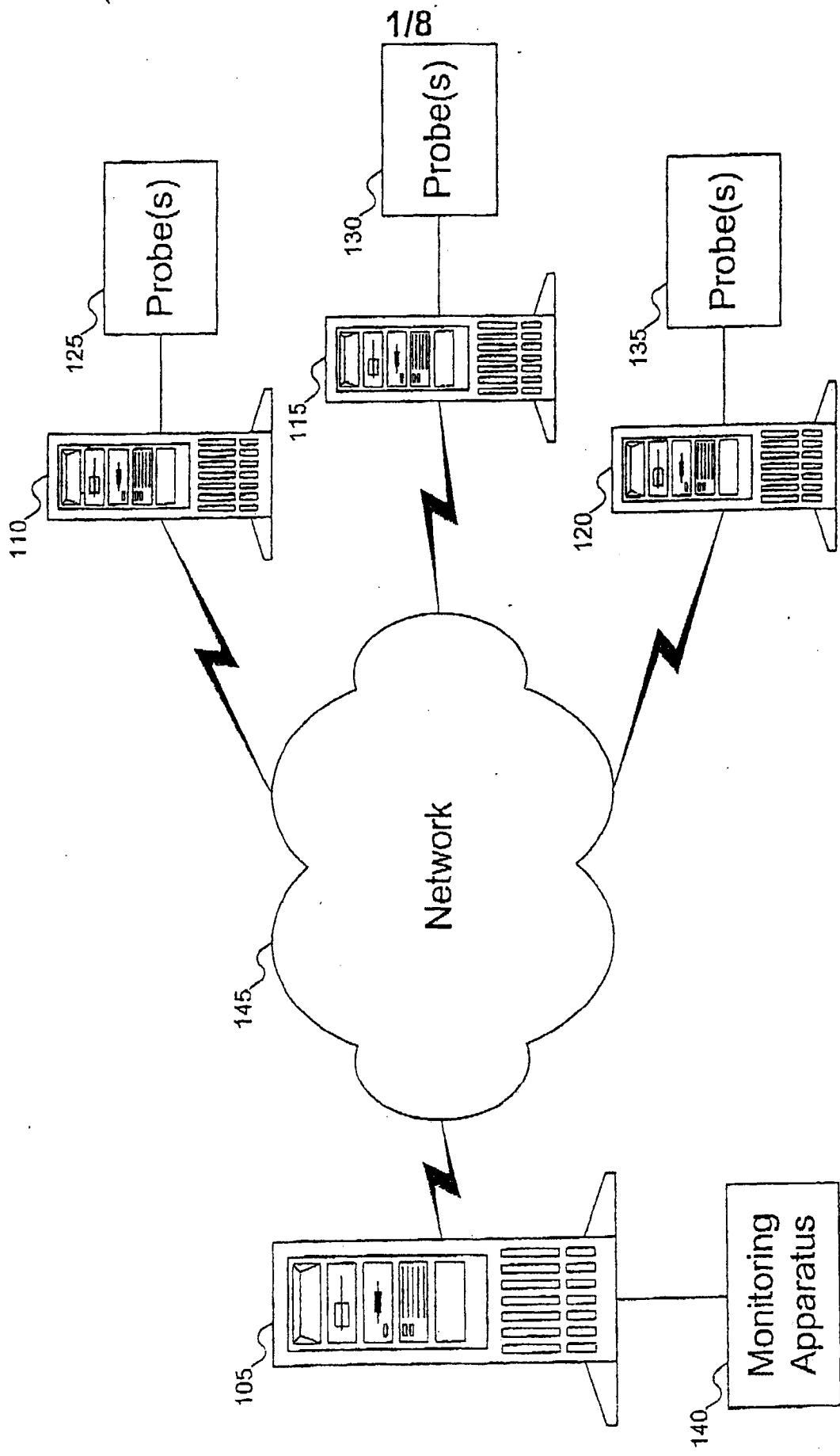


FIG. 1

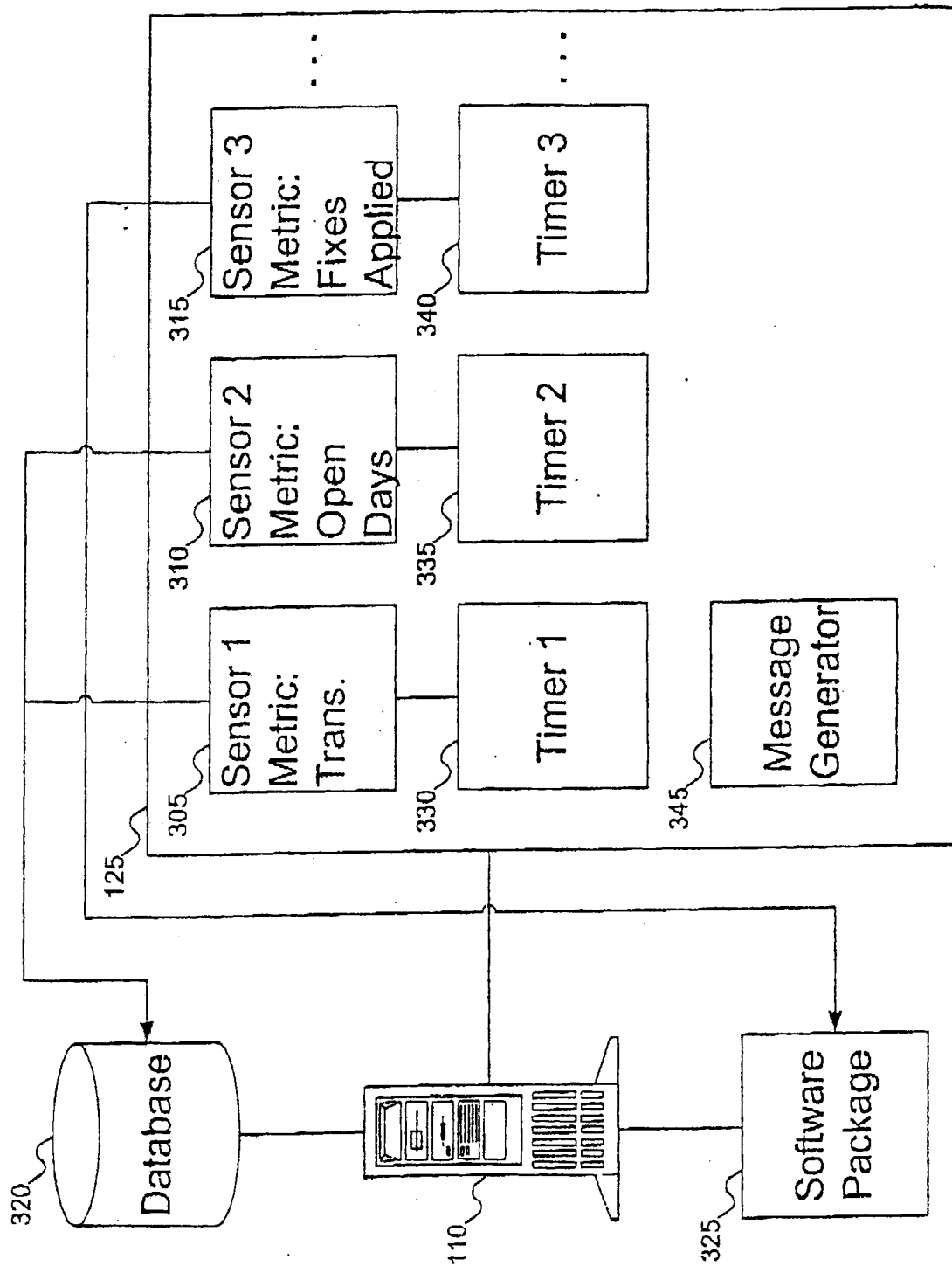


FIG. 3

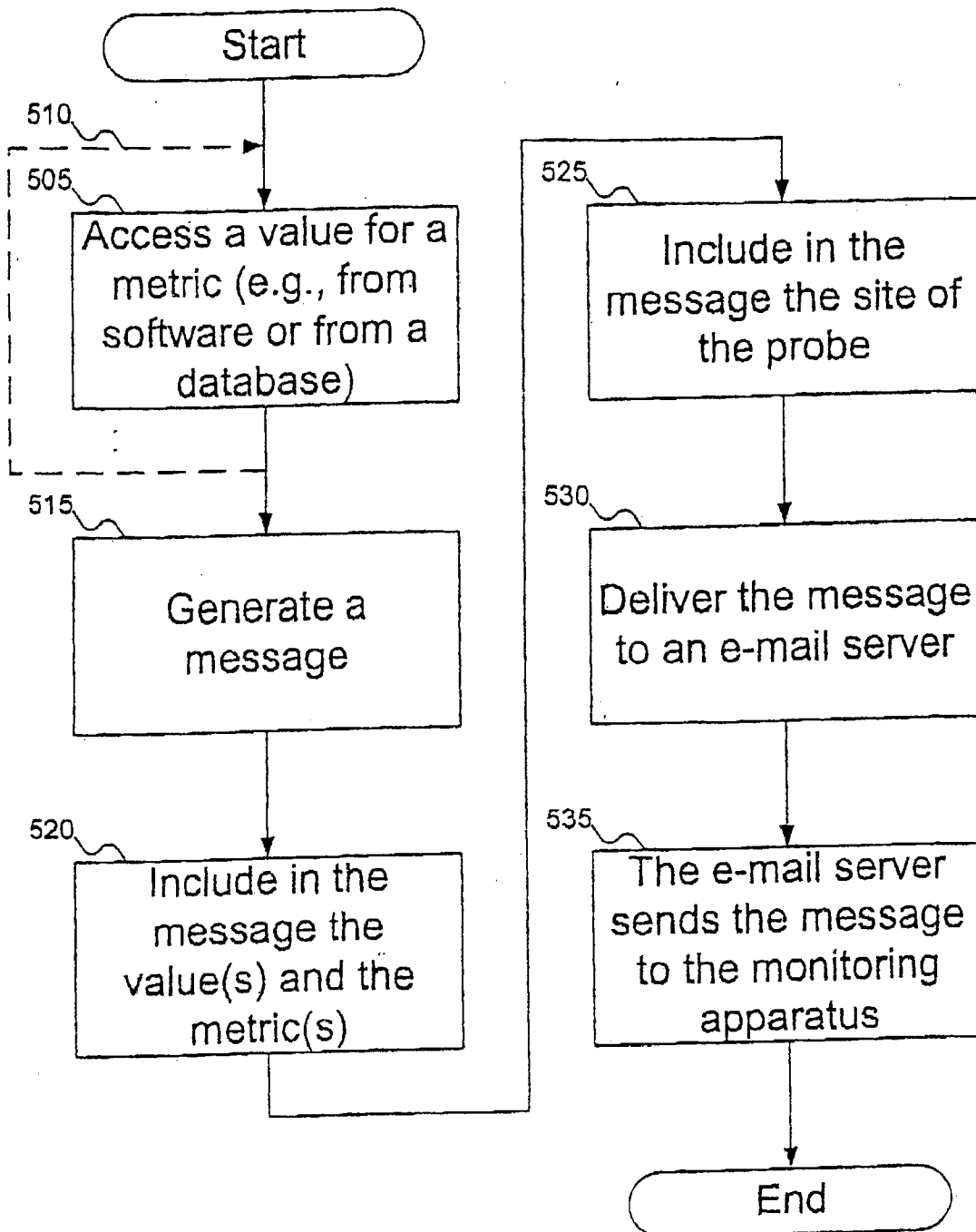


FIG. 5

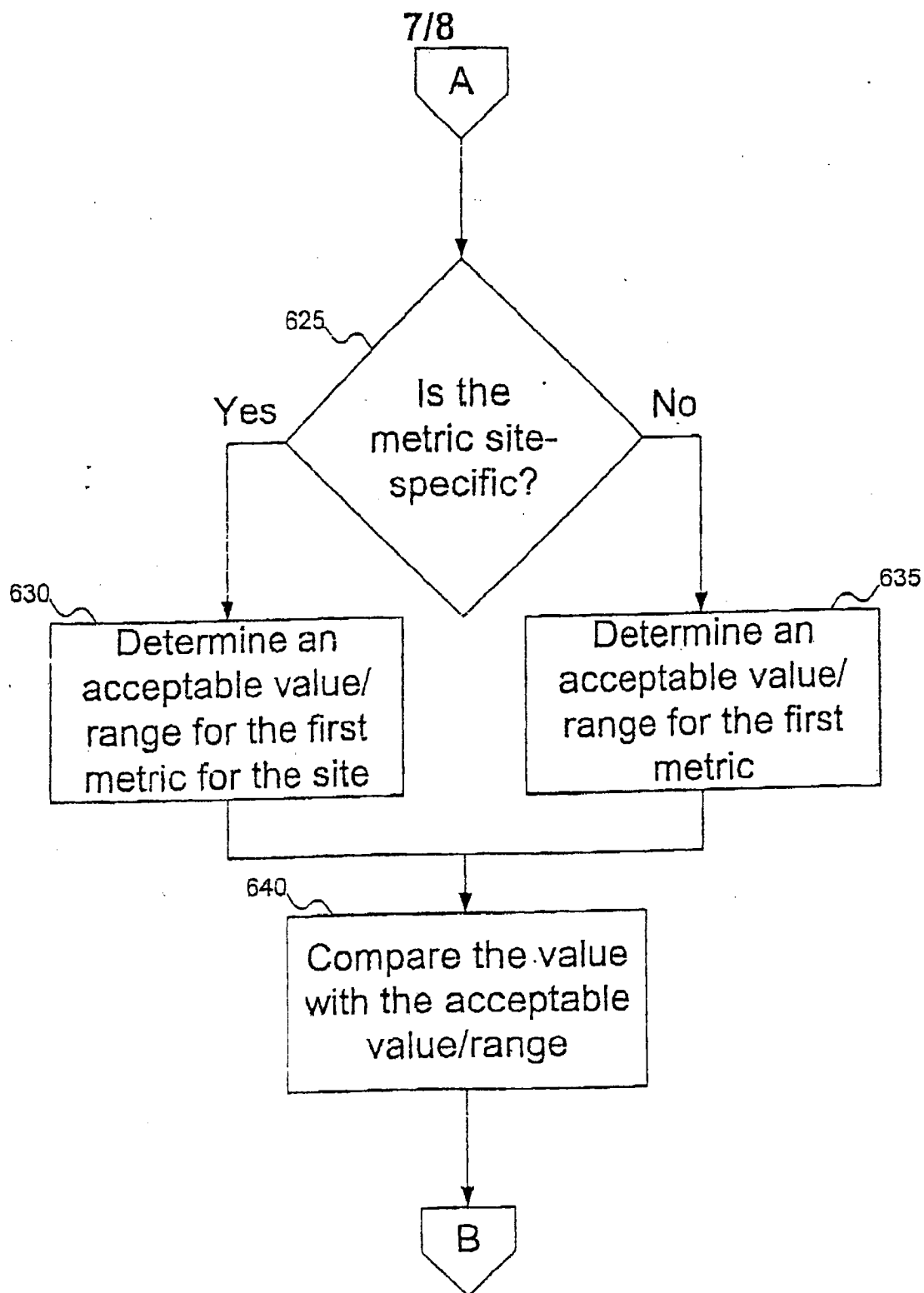


FIG. 6B

**METHOD AND APPARATUS FOR MONITORING AND UPDATING SYSTEM  
SOFTWARE**

**FIELD OF THE INVENTION**

This invention pertains to monitoring software for a variety of conditions such as internal performance characteristics, liability warnings, programmatic errors and the general health of the computer system.

**BACKGROUND OF THE INVENTION**

No matter the computer program, it is inevitable that there will be some bugs (that is, coding errors that cause the program to behave differently what is expected). Production environments represent a number of variables that are difficult to reproduce in testing environments. As such, applications with thousands of interfaces can fail under a variety of changing variables.

Because human intervention is required to maintain these applications, certain tasks must be completed by operations on a timely basis. Failure to operate and maintain the system within the published guidelines for the application will result in a number of unacceptable issues. These include, but are not limited to the following: inaccurate reporting of revenues; increased risks associated with liability; increased risks with system availability; and increased costs due to additional manpower correction activities.

Customers want to know that their mission critical system is performing at peak levels of performance. They want to know when an area of the system is failing. They need to feel confident that the system and its integration with operations are running smoothly. Not knowing the health of the internal components of the system can create a false sense of security

Another thing software companies sometimes do to eliminate defects is to find out about defects from customers. For a long time, customers had to make contact with the software companies (either by telephone or by e-mail) and let the software companies know about the bugs. More recently, as exemplified by Microsoft® Windows® XP, the operating system offers to send an error report to the software company when a program crashes. That

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 shows a central server with a monitoring apparatus, communicating with probes on customer computers, according to an embodiment of the invention. In FIG. 1, server 105 is a central server. Server 105 is operated by the company distributing software products to its customers. Customers operate, for example, computers 110, 115, and 120. Although a person skilled in the art will recognize that there can be more or fewer than three customers, and that each customer can have more than one computer.

Installed on computers 110, 115, and 120 are probes 125, 130, and 135. Probes 125, 130, and 135 are responsible for determining the values associated with various metrics on computers 110, 115, and 120 respectively, and transmitting these values back to server 105. The details of probes 125, 130, and 135 are discussed further with reference to FIGs. 3-4 below.

Server 105 includes monitoring apparatus 140. Monitoring apparatus 140 receives information from probes 125, 130, and 135, and determines whether the data received from the probes represent acceptable values. If the values are acceptable, then monitoring apparatus 140 logs the values. Otherwise, monitoring apparatus displays 140 an alert, indicating the unacceptable value. The details of monitoring apparatus 140 are discussed further with reference to FIG. 2 below.

Connecting server 105 with computers 110, 115, and 120 is network 145. Network 145 can be any variety of network including, among others, a local area network (LAN), a wide area network (WAN), a global network (such as the Internet), and a wireless network (for example, using Bluetooth or any of the IEEE 802.11 standards). In addition, a person skilled in the art will recognize that different networks can be used to connect server 105 with different computers. For example, server 105 might be connected to computer 110 using one network, and to computers 115 and 120 using a second network.

FIG. 2 shows details of the monitoring apparatus of FIG. 1. Monitoring apparatus 140 includes four components: receiver 205, tester 210, alerter 215, and log 220. Receiver 205 is responsible for receiving a message from a probe and parsing the message for the necessary information. Tester 210 then tests the value (or values) retrieved from the message received by receiver 205 to determine if the value is acceptable. Alerter 215 displays an alert is the value retrieved from the message is not acceptable. And log 220 includes entries, like

Because sensor measurements are taken more than once, each of sensors 305, 310, and 315 includes a corresponding timer 330, 335, and 340. The timers ensure that the sensors take measurements according to regular schedules. Each timer can be set to measure a metric using different intervals. But a person skilled in the art will recognize that, for sensors  
5 measuring metrics according to consistent schedules, a single timer can be used for more than one sensor.

Additionally, sensors can trigger on two different mechanisms. They can be triggered on a timer or they can be triggered by an impromptu event. The latter is utilized to signal immediate attention to a critical event that has just taken place.

10 Finally, probe 125 includes message generator 345. Message generator 345 takes the measurements from the various sensors 305, 310, and 315, and assembles a message from the measurements. The message is then sent to the central server (not shown in FIG. 3). Message generator 345 can generate a single message for several metric measurements, or message generator 345 can generate a separate message for each metric measurement.

15 FIG. 4 show the probes of FIG. 1 communicating with the monitoring apparatus of FIG. 1. In FIG. 4, message generator 345 is shown generating message 405. Message 405 is shown in greater detail in blow-up 410. The message is dated August 7, 2003, and is from site 1 (which includes computer 110). Blow-up 410 shows two metric measurements. The site has measured 500,000 transactions, and has five open days. There can also be other  
20 metrics included in the message.

Once message 405 is generated, it is delivered to e-mail server 415. E-mail server is responsible for starting message 405 along its journey to receiver 205 in the central server. Although shown as a component of computer 110, a person skilled in the art will recognize that e-mail server 415 can be part of a separate computer, distinct from computer 110, or can  
25 be a dedicated e-mail server. A typical implementation would most likely utilize the customer's existing e-mail implementation. This will provide a number of benefits including a cost savings through the elimination of a second server along with cost avoidance of supporting and maintaining the additional hardware.

FIG. 5 shows a flowchart of the procedure for using the probes of FIG. 1. At step  
30 505, the probe accesses a value for a metric. The value can be accessed from a database or from software. As shown by arrow 510, step 505 can be repeated as often as necessary, to access values for multiple metrics. At step 515, a message is generated. At step 520, the message includes the value for the metric accessed in step 505. At step 525, the site is



can be modified in arrangement and detail without departing from such principles. All modifications coming within the spirit and scope of the accompanying claims are claimed.

9. A monitoring apparatus according to claim 8, wherein:

the tester includes a first filter, the first filter defining a range of acceptable values for the first metric; and

5 the tester is operative to compare the first value with the range of acceptable values for the first filter.

10. A monitoring apparatus according to claim 9, wherein the tester includes:

a plurality of filters, each filter determining a range of acceptable values for a metric;

10 and

a selector to select the first filter from the plurality of filters based on the first metric in the first message.

11. A monitoring apparatus according to claim 10, wherein:

15 the plurality of filters includes at least one filter defining a range of acceptable values for the first metric associated with a site; and

a selector to select the first filter from the plurality of filters based on a first site in the first message.

20 12. A monitoring apparatus according to claim 8, further comprising a log, the log including an entry corresponding to the first message.

13. A system for monitoring software, comprising:

a central computer;

25 a monitoring apparatus installed in the central computer;

a first computer;

a first probe installed in the first computer; and

a network connecting the central computer and the first computer.

30 14. A system according to claim 13, where:

the system further comprises:

a second computer; and

a second probe installed in the second computer; and

21. A method according to claim 19, wherein accessing the first value includes accessing a software package by the probe.

5 22. A method according to claim 19, wherein accessing the first value includes accessing a database by the probe.

23. A method according to claim 19, wherein generating a message further includes generating the message by the probe, the message including the first value for the  
10 first metric and an identifier for a site of the probe.

24. A method for using a monitoring apparatus, comprising:  
receiving a message;  
determining a first value for a first metric from the message;  
15 determining if the first value for the first metric is acceptable; and  
if the first value for the first metric is not acceptable, displaying an alert that the first value for the first metric is not acceptable.

25. A method according to claim 24, further comprising, if the first value for the  
20 first metric is acceptable, logging the first value for the first metric.

26. A method according to claim 24, wherein:  
determining a first value includes determining the first value for the first metric for a first site from the message; and  
25 determining if the first value for the first metric is acceptable includes determining if the first value for the first metric for the first site is acceptable.

27. A method according to claim 24, wherein determining if the first value for the first metric is acceptable includes comparing the first value for the first metric with at least  
30 one acceptable value.

software to deliver the message to the monitoring apparatus by the e-mail server.

36. Computer-readable media according to claim 34, wherein the software to access the first value includes software to access a software package by the probe.

37. Computer-readable media according to claim 34, wherein the software to access the first value includes software to access a database by the probe.

38. Computer-readable media according to claim 34, wherein the software to generate a message further includes software to generate the message by the probe, the message including the first value for the first metric and an identifier for a site of the probe.

39. Computer-readable media containing a program to use a monitoring apparatus, the program comprising:

software to receive a message;  
software to determine a first value for a first metric from the message;  
software to determine if the first value for the first metric is acceptable; and  
if the first value for the first metric is not acceptable, software to display an alert that the first value for the first metric is not acceptable.

40. Computer-readable media according to claim 39, further comprising, if the first value for the first metric is acceptable, software to log the first value for the first metric.

41. Computer-readable media according to claim 39, wherein:  
the software to determine a first value includes software to determine the first value for the first metric for a first site from the message; and  
the software to determine if the first value for the first metric is acceptable includes software to determine if the first value for the first metric for the first site is acceptable.

42. Computer-readable media according to claim 39, wherein the software to determine if the first value for the first metric is acceptable includes software to compare the first value for the first metric with at least one acceptable value.

49. A probe apparatus or a monitoring apparatus, or a system for monitoring software constructed and arranged to operate substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.

5 50. A method of using a monitoring apparatus substantially as hereinbefore described with reference to and as illustrated in the accompanying drawings.



Application No: GB0420423.6

Examiner: Dr Stephen Richardson

Claims searched: 1-7, 19-23, 34-38

Date of search: 21 December 2004

## Patents Act 1977: Search Report under Section 17

### Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X,E	1-7, 19-23, 34-38	WO 2004/088604 A1 (ACRES GAMING) see Figures 2-4 and page 8, line 8 to page 18, line 12.
X	1-7, 19-23, 34-38	WO 00/65448 A1 (UNIVERSAL MUSIC) see Figures 2a, 2b and page 4, lines 15-30.
X	1-7, 19-23, 34-38	US 5796633 A (ELECTRONIC DATA SYSTEMS) see whole document, in particular abstract and summary of the invention.
X	1-7, 19-23, 34-38	US 6636983 B1 (LEVI) see Figure 11 and column 21, line 35 to column 22, line 5.
X	1-7, 19-23, 34-38	WO 2003/090085 A2 (COMPUTER ASSOCIATES THINK) see whole document.
X	1-7, 19-23, 34-38	US 5726912 A (HONEYWELL) see whole document.

### Categories:

X Document indicating lack of novelty or inventive step	A Document indicating technological background and/or state of the art.
Y Document indicating lack of inventive step if combined with one or more other documents of same category.	P Document published on or after the declared priority date but before the filing date of this invention.
& Member of the same patent family	E Patent document published on or after, but with priority date earlier than, the filing date of this application.

### Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC<sup>W</sup> :

Worldwide search of patent documents classified in the following areas of the IPC<sup>07</sup>

G06F